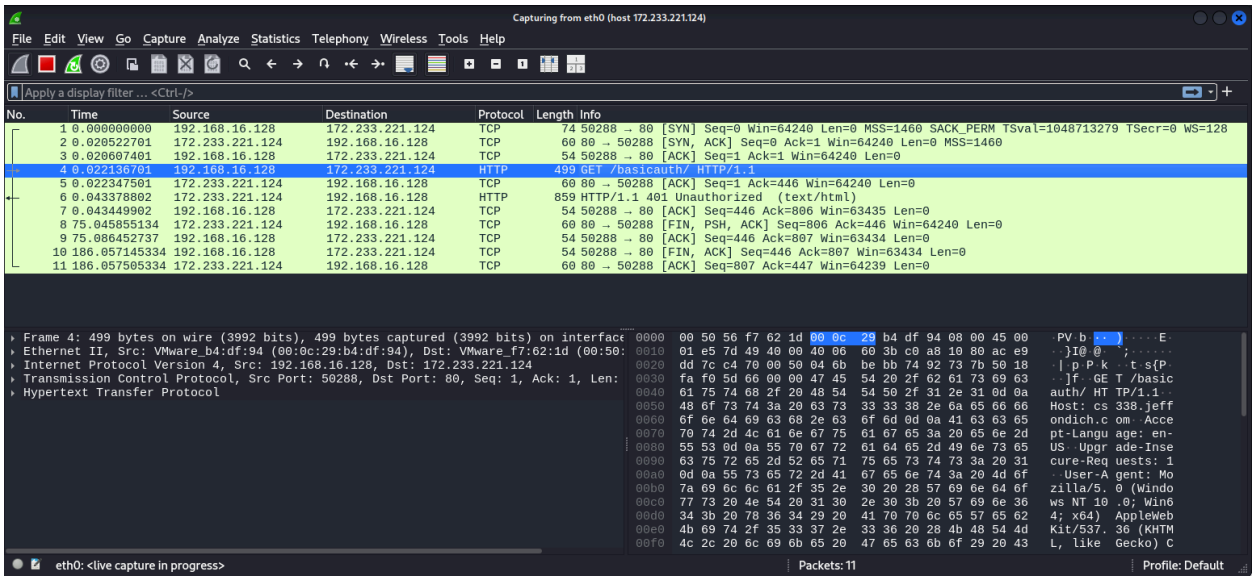
Ntenese Obono and Ugo Anyaegbunam

Command to get link IP address: curl -v cs338.jeffondich.com

Use Wireshark to filter the host by its IP address. Packet sniffing is just looking at the packets where interactions happen. This shows the client-server interactions.

Steps:

1.) We ran this command " curl -v cs338.jeffondich.com" to get the link IP address:
2.) The first GET request is sent and it looks like this:



GET /basicauth/ HTTP/1.1
Host: cs338.jeffondich.com
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

3.) After we finished the interception on burp suite, we noticed that what was originally a 200 request the title changed to "401 Authorization Required," which we imagine is the login username and

password. Then we noticed in burp suite that the server tells us the client that we need to be authorized for access.

a.) We also see a TCP handshake in Wireshark and after the TCP handshake, we see the server acknowledge the request and respond that we are unauthorized. It lets us know that it's finished sending data and wants to close the connection, and the PSH flag is telling us to process the data right away and not buffer it. Then it acknowledges that we received the data

b.) We send back an acknowledgement to the server that we got the data, and we also acknowledge that we want to close the connection to the server. Lastly, the server acknowledges our request and closes the connection, which explains the intercept turning off.

At this time, 11 packets have been sent, and 1 request has been made.

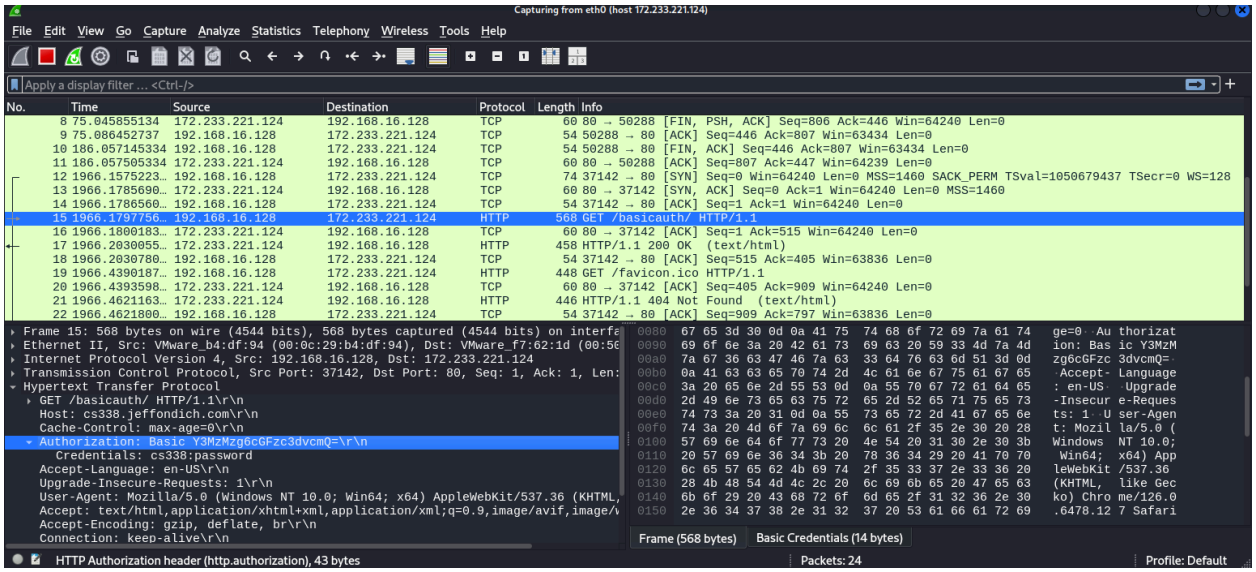
After the password is typed by the user, what sequence of queries and responses do you see?

4.) **Sign in:** After entering the credentials, another GET request was made, and we got a 200 status code in Burp Suite, which is a successful connection.

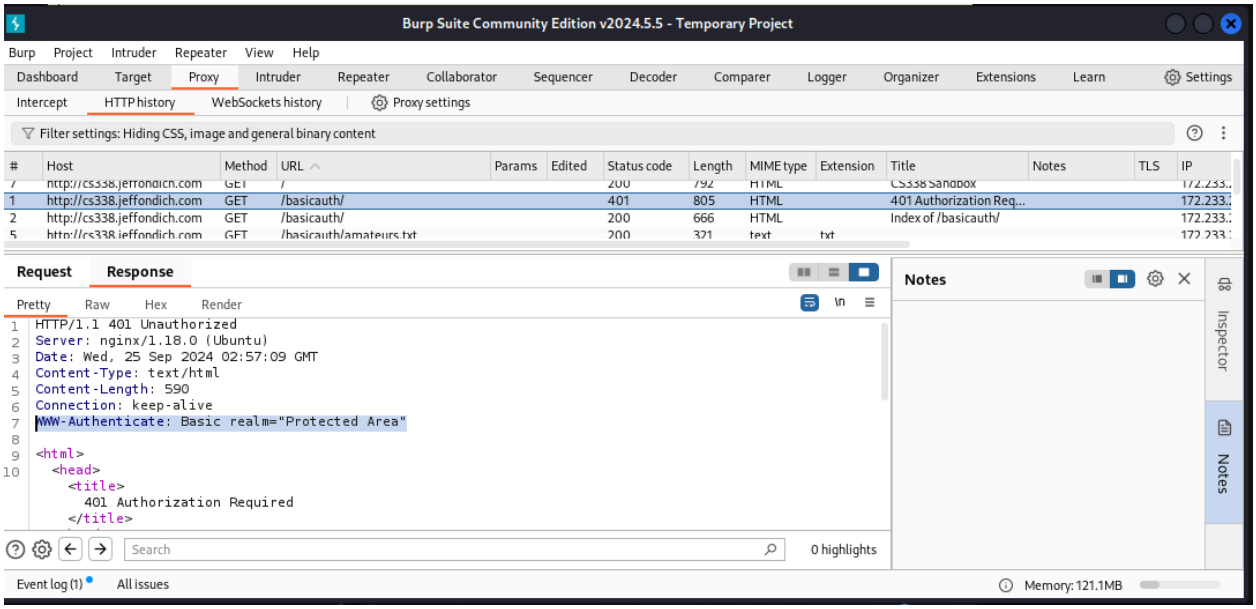
5.) In Wireshark, we see a TCP handshake, then we see the HTTP protocol making a GET request to /basicauth/. After the TCP handshake, we see the frame representing the server at the path /basicauth/. The server gives us a 200 response, acknowledging that it successfully received our request.

Is the password sent by the browser to the server, or does the browser somehow do the password checking itself? If the former, is the password sent in clear text or is it encrypted or something else?

6.) Then we observe within our GET request an authorization header containing our credentials as well as the type of authorization. The authorization header is used to send credentials to the server for authentication. We see that our basic authentication header contains a base64 encoded string as seen in the figure below sent by the client to the server, which is then decoded by the server as the username and password separated by a colon. The encrypted key comes from the client



Connected to the documentation, we see Basic, which is the authentication scheme they mention. We also know that the 401 for sure is telling us that authentication is required as mentioned in the documentation. We also learned via the documentation that these status codes are related to the HTTP/1.1 protocol, which is the protocol we see used in many of our requests. Furthermore, we also observed the www-authenticate header in the response, which is mandated as mentioned in 3.1 of the documentation.



7.) Then we observe our client making a GET request for the server, and many browsers make this request by default. However, we get a 404 not found because the server doesn't have one.
8.) We then observe the same 3 frames, ACK, FIN, PSH, signaling the end of the conversation from both the server and client.